NUREG-0800

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

APPENDIX 7-B - ACRONYMS, ABBREVIATIONS, AND GLOSSARY

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

A. ACRONYMS AND ABBREVIATIONS

AFW	auxiliary feedwater
ALWR	advanced light water reactor
AMI	accident monitoring instrumentation
ANS	American Nuclear Society
ANSI	American National Standards Institute
ARI	alternate rod injection
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
B&W	Babcock and Wilcox
BISI	bypassed or inoperable status indication
BTP	branch technical position
BWR	boiling water reactor
BWROG	boiling water reactor owners' group
CDF	core damage frequency
CDM	certified design material
CE	Combustion Engineering

USNRC STANDARD REVIEW PLAN

This Standard Review Plan, NUREG-0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The Standard Review Plan is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The standard review plan sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of Regulatory Guide 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on Regulatory Guide 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by email to NRR_SRP@nrc.gov.

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, or by fax to (301) 415-2289; or by email to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC's public Web site at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading-rm/adams.html, under Accession # ML070660430.

CFR	Code of Federal Regulations
CLA	combined license application
CM	configuration management
COL	combined license or combined operating license
Common Q	Westinghouse common qualified
COTS	commercial off-the-shelf
CP	construction permit
D3	diversity and defense-in-depth
DAC	design acceptance criteria
DAS	diverse actuation systems
DC	design certification
DCD	design certification document
DCS	data communication system
ECCS	emergency core cooling system
EEPROM	electrically erasable programmable read-only memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EPRI	Electrical Power Research Institute
ERDS	Emergency Response Data System
ERF	emergency response facility
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESP	early site permit
FR	Federal Register
FSAR	final safety analysis report
FSER	final safety evaluation report
GDC	general design criteria(on)
GSI	generic safety issue
HVAC	heating, ventilation, and air conditioning
I/O	Input/output
I&C	instrumentation and control
ICS	integrated control system
ICT	installation configuration table
IEC	International Electrotechnical Commission
IEEE	Institute of Electronic and Electrical Engineers
ISA	International Society for Measurement and Control (formerly Instrument Society of America)
ISO	International Standards Organization
ITAAC	inspection, test, analysis, and acceptance criteria
IV&V	independent verification and validation
LCSR	loop current step response
LERF	large early release frequency
LSP	limiting set point
LSSS	limiting safety system setting
LWR	light water reactor
MCF	maximum credible fault
MCR	main control room
MOIV	motor-operated isolation valve
NRC	Nuclear Regulatory Commission
NRO	Office of New Reactors
NRR	Office of Nuclear Reactor Regulation

OL	operating license
OM	operations manual
OMB	Office of Management and Budget
PAM	post-accident monitoring
PDS	pre-developed software
PLC	programmable logic controller
PRA	probabilistic risk assessment
PSAR	preliminary safety analysis report
PWR	pressurized water reactor
QA	quality assurance
RAI	request for additional information
RCS	reactor coolant system
RFI	radio frequency interference
RHR	residual heat removal
RPS	reactor protection system
RTD	resistance temperature detector
RTM	requirements traceability matrix
RTS	reactor trip system
SAD	software architecture description
SAR	safety analysis report
SBD	system build document
SCM	software configuration management
SCMP	software configuration management plan
SDP	software development plan
SDS	software design specifications
SECY	commission paper
SER	safety evaluation report
SIntP	software integration plan
SInstP	software installation plan
SLCS	standby liquid control system
SMaintP	software maintenance plan
SMM	software maintenance manual
SMP	software management plan
SOP	software operations plan
SPDS	safety parameter display system
SQAP	software quality assurance plan
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SRS	software requirements specifications
SRV	safety relief valve
SSAR	standardized safety analysis report
SSCs	systems, structures, and components
SSP	software safety plan
Std	standard
STM	software training manual
STP	software test plan
STrngP	software training plan
SVVP	software verification and validation plan
SWC	surge withstand capability
TMI	Three Mile Island
TP	test plan

TR	topical report
USI	unresolved safety issue
V&V	verification and validation
VDU	video display unit

B. GLOSSARY

Acceptance criteria - Criteria which, when met, ensures acceptable compliance with the relevant requirements of NRC's regulations.

Accuracy - The degree of freedom from error of sensor and operator input, the degree of exactness exhibited by an approximation or measurement, and the degree of freedom from error of actuator output.

Activity group - A collection of software life cycle activities, all of which are related to a specific life cycle topic. Eight activity groups are recognized in SRP BTP 7-14: planning, requirements, design, implementation, integration, validation, installation, and operations and maintenance.

Activity - A group of related tasks [IEEE Std 1074].

Auxiliary supporting features and other auxiliary features - Typically are electric power systems, diesel generator fuel storage and transfer systems, instrument air systems, HVAC systems for ESF areas, and essential service water and component cooling water systems. Figure 3 of IEEE Std 603-1991, "Examples of Equipment Fitted to Safety System Scope Diagram," provides a matrix with an extensive list of auxiliary supporting features and other auxiliary features.

Commission Papers - Written issues papers the NRC staff submits to the Commission to inform them about policy, rule making, and adjudicatory matters.

Completeness - Those attributes of the design outputs that provide full implementation of the functions required of the software. The functions which the software is required to perform are derived from (1) the general functional requirements of the safety system, and (2) the assignment of functional requirements to the software in the overall system design.

Configuration control board - The authority responsible for evaluating and recommending disposition of proposed changes.

Configuration management - A discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements [610.12].

Consistency (as a software functional characteristic) - The degree of freedom from contradiction among the different documents and components of a software system. Internal consistency denotes the consistency within the different parts of a component; for example, a software design is internally consistent if no set of design elements are mutually contradictory. External consistency denotes the consistency between one component and another; for example, software requirements and the resulting code are consistent with one another if there are no contradictions between the requirements and the code.

Control systems - Those systems used for normal operation that are not relied upon to perform safety functions following anticipated operational occurrences or accidents. The control systems evaluated using SRP Chapter 7 are those which control plant processes having a significant impact on plant safety, but are not wholly incorporated into systems addressed by other SRP chapters.

Correctness - The degree to which a design output is free from faults in its specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.

Critical characteristics - Properties or attributes that are essential for performance of an equipment's safety function. [IEEE Std 934-1987]

Data communication systems (DCS) - Systems that transmit signals between systems and between components of systems. Data communication systems may include analog and digital multiplexers as well as non-multiplexed transmission. Where such systems are included in a design, they support one or more of the I&C systems.

Design acceptance criteria (DAC) - A set of prescribed limits, parameters, procedures, and attributes upon which the NRC relies in making a final safety determination to support design certification when detailed design information is not available. The DAC are part of the Tier 1 information.

Design certification document (DCD) - The master document that contains the information that is referenced by the design certification rule. The DCD includes both the Tier 1 information that is certified by the design certification rule and the Tier 2 information that is approved by and supports the rule. The DCD is composed of the certified design material and the non-proprietary version of the SAR, including all material incorporated by reference.

Design margin - The additional performance capability above required standard basic system parameters that may be specified by a system designer to compensate for uncertainties.

Design process - Technical and management process that commence with identification of design input and lead to and include the issuance of design output documents. [ASME Std NQA-1-1994]

Design output - Documents, such as drawings and specifications, that define technical requirements of structures, systems, and components (ASME Std NQA-1, "Quality Assurance Requirements for Nuclear Facility Applications"). For software, design outputs are the products of the development process that describe the end product that will be installed in the plant. The design outputs of a software development process include software requirements specifications, software design specifications, hardware and software architecture designs, code listings, system build documents, installation configuration tables, operations manuals, maintenance manuals, and training manuals.

Design requirement - Specification or constraints on the design of a system or system component. [IEEE Std 610.12-1990]

Deterministic timing - Timing is deterministic if the time delay between stimulus and response has a guaranteed maximum and minimum.

Differential Modes - Faults between the signal terminals that cause the potential of one side of the signal transmission path to be charges relative to the other side.

Direct indication - Indication from direct measurement of desired variable.

Diverse instrumentation and control systems (diverse I&C). Those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.”

Documentation - Information recorded about a specific life cycle activity. Forty-one activities are recognized in SRP BTP 7-14. Documentation includes software life cycle design outputs and software life cycle process documentation. A document may be in written or electronic format, and may contain text, illustrations, tables, computer files, program listings, binary images, and other forms of expression. A document for an activity may be divided into several individual entities.

Embedded software or firmware - Software that is built into (stored in read-only memory) a computer dedicated to a pre-defined task. Normally, embedded software cannot be modified by the computer that contains it, nor will power failure erase it; some computers may contain embedded software stored in electrically erasable programmable read-only memory (EEPROM), but changing this memory typically requires a special sequence of actions by maintenance personnel.

Engineered safety features (ESF) - Safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release, which are cladding, reactor coolant pressure boundary, and containment.

Engineered safety features actuation systems (ESFAS) - Those I&C systems which initiate and control safety equipment which removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, reactor coolant pressure boundary, and containment).

Formal methods - Mathematically based methods for the specification, design, and production of software. Also includes a logical inference system for formal proofs of correctness, and a methodological framework for software development in a formally verifiable way [MOD-00-55].

Function - Specific purpose of an entity or its characteristic action. [IEEE Std 610.12-1990]

Functional characteristic - A trait or property of a design output that implements a functional requirement, a portion of a functional requirement, or a combination of functional requirements. For software, functional characteristics include accuracy, functionality, reliability, robustness, safety, security, and timing.

Functional requirement - A requirement that specifies a function that a system or system component must be capable of performing [IEEE Std 610.12]. In the SRP, the term functional requirement includes design requirements, interface requirements, performance requirements, and physical requirements.

Functionality (as a software functional characteristic) - Those operations which must be carried out by the software. Functions generally transform input information into output information in order to affect the reactor operation. Inputs may be obtained from sensors, operators, other equipment, or other software. Outputs may be directed to actuators, operators, other equipment, or other software.

Handshake - A four-step process of linked acknowledgments between a sender and a receiver used to transmit data or signals reliably. A handshake involves a signal that (1) initiates the transaction (from the initiating member of a pair), (2) accepts the transaction (from the passive member), (3) terminates the transaction (from the initiator), and (4) acknowledges the termination and readiness for another transaction (from the passive member).

Hardware critical characteristics - Properties or attributes of computer, peripheral, or communication hardware that are essential for performance if the safety function, including specifications that are required to execute the software intended to run on the hardware and the attributes of reliability, testability, or predictability, on which the staff's safety findings are based.

Implementation (as a software life cycle process planning characteristic) - Those characteristics of planning documents that describe the work necessary to achieve the purpose of the planning documents. The implementation characteristics of software life cycle plans discussed in SRP BTP 7-14 are: measurement, procedures, record keeping, and schedule.

Information systems important to safety - Those systems which provide information to the operators for the safe operation of the plant during normal operation, anticipated operational occurrences, and accidents. The information systems important to safety include those systems which provide information for manual initiation and control of safety systems. They indicate that plant safety functions are being accomplished and provide information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences and accidents. During normal plant operation, the information systems important to safety provide information on the normal status and the bypassed and inoperable status of safety systems.

Integration - The process of combining system entities into an overall functioning system.

Interface - A shared boundary across which information is passed [IEEE Std 610.12].

Interlock systems important to safety - Those systems which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident. These systems differ from protection systems in that interlock system safety action is taken prior to or to prevent accidents.

Interrupt - The suspension of a process to handle an event external to the process.

Management (as a software life cycle process planning characteristic) - Those characteristics of planning documents that are primarily significant to the managing of the project activities described in the planning document. The management characteristics of software life cycle plans discussed in SRP BTP 7-14 are: purpose, organization, oversight, responsibilities, risks, and security.

Maximum credible fault (MCF) - A voltage or current transient that may exist in circuits, as determined by test or analysis, taking into consideration the circuit location, routing, and interconnections combined with failures that the circuit may credibly experience.

On-line testing - Testing performed on an operable system.

Operable - A system, subsystem, train, component, or device is operable when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its specified safety function(s) are also capable of performing their related support function(s).

Performance - The degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage [IEEE Std 610.12].

Periodic tests - Tests performed at scheduled intervals to detect failures and verify operability [IEEE Std 338]. Periodic tests include surveillance tests.

Predeveloped software (PDS) - Software that already exists, is available as a commercial or proprietary product, and is being considered for use in a computer-based function [IEC Std 880, Supplement 1 draft]. Commercial off-the-shelf (COTS) software is a subset of PDS.

Protection systems - Those I&C systems which initiate safety actions to mitigate the consequences of design basis events. The protection systems include the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS).

Reactor trip systems (RTS) - Those I&C systems that initiate rapid control rod insertion to mitigate the consequences of design basis events.

Reliability (as a software functional characteristic) - The degree to which a software system or component operates without failure. This definition does not consider the consequences of failure, only the existence of failure.

Redundancy - Multiple SSC's each capable of performing a given function.

Requirements Traceability Matrix (RTM) - An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement.

Resources (as a software life cycle process planning characteristic) - The material resources necessary to carry out the work defined in the planning document. The resource characteristics of software life cycle plans discussed in SRP BTP 7-14 are: budget, methods/tools, personnel, and standards.

Robustness (as a software functional characteristic) - The ability of a software system or component to function correctly in the presence of invalid inputs or stressful environmental conditions. This includes the ability to function correctly despite some violation of the assumptions in its specification.

Safe shutdown systems - Those systems which function to achieve and maintain a safe shutdown condition of the plant. The safe shutdown systems include those I&C systems used to maintain the reactor core in a subcritical condition and provide adequate core cooling to achieve and maintain both hot and cold shutdown conditions.

Safety (as a software functional characteristic) - Those properties and characteristics of the software system that directly affect or interact with system safety considerations. The safety characteristic is primarily concerned with the effect of the software on system hazards and the measures taken to control those hazards.

Safety systems - Those systems that are relied upon to remain functional during and following design basis events to assure the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures.

Security - The ability to prevent unauthorized, undesired, and unsafe intrusions.

Self-test - A test or series of tests, performed by a device upon itself. Self-test includes on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics.

Software critical characteristics - Properties or attributes of a software or firmware product that is essential for performance if the related equipment's safety function. Characteristics include functional requirements that are allocated to the software and the attributes of robustness, testability, or dependability, on which the staff's safety findings are based.

Software development process characteristic - A trait or property of a software development process design output that results from the implementation of a design process, including completeness, consistency, correctness, style, traceability, unambiguity, and verifiability.

Software development requirement - One or more activities that a software development process must include.

Software life cycle - A project-specific, time-sequenced mapping of activities [IEEE Std 1074].

Staff Requirements Memorandum (SRM) - The Commission's decisions and directions to the staff on the issues discussed in the associated SECY. SRMs also are issued following each Commission meeting to document any discussion or request made at the meeting.

Style (as a software functional characteristic) - The form and structure of a design output. Document style refers to the structure and form of a document. This has connotations of understandability, readability, and modifiability. Programming style refers to the programming language characteristics of the software.

Surveillance tests - Tests conducted specifically to confirm compliance with technical specification surveillance requirements.

Task - The smallest unit of work subject to management accountability. A task is a well-defined work assignment for one or more project members [IEEE Std 1074].

Testability - (1) The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met [610.12]. (2) The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met [IEEE Std 610.12].

Tier 1 - The design-related information contained in the DCD that constitutes the certified standard design. This information identifies the scope of the standard design and consists of the certified design descriptions, the ITAAC, the site parameters, and the interface requirements. Tier 1 material becomes part of the design certification rule and may be changed only by rule-making.

Tier 2 - The design-related information contained in the DCD that is not Tier 1 information. It supports the certification of a standard design by providing additional details about the proposed implementation. The Tier 2 information generally consists of the SAR with the proprietary information removed for purposes of rule-making. Although Tier 2 information is not certified by the design certification rule, it consists of “those matters resolved in connection with the issuance or renewal of a design certification” within the meaning of 10 CFR 52.63(a)(4). Tier 2 material is approved by the design certification rule, but is not part of the rule. Tier 2 material may be changed by a process similar to that described in 10 CFR 50.59, unless designated as Tier 2* in the SER.

Tier 2* - A subset of Tier 2 material that the NRC SER and DCD for the standardized plant design approval identifies as requiring NRC approval prior to modification or change by the applicant/licensee.

Timing (as a software functional characteristic) - The ability of the software system to achieve its timing objectives within the hardware constraints imposed by the computing system being used.

Traceability - The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backward to one or more elements of a predecessor life cycle product.

Unambiguity - The degree to which each element of a life cycle product, and of all elements taken together, have only one interpretation.

Unbounded loop - The term used to describe the situation in which a programming language control structure called a loop has no upper limit to the number of times it may execute.

Validation - The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements [IEEE Std 610.12].

Verifiability (as a software functional characteristic) - The degree to which a software design output is stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses, reviews, or tests to determine whether those criteria have been met.

Verification and Validation (V&V) - The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements [IEEE Std 610.12].

Verification - The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase [IEEE Std 610.12].

Walkthrough - A static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a segment of documentation or code, and the participants ask questions and make comments about possible errors, violation or development standards, and other problems. [IEEE Std 610.12]

Watchdog timer - A form of interval timer that is used to detect a possible malfunction and is typically arranged to cause a hardware restart if not reset periodically by software.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval number 3150-0011 and 3150-0151.

PUBLIC PROTECTION NOTIFICATION

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.